Maturing Aspects of Internet Security

The information security picture is changing. Threats are expanding. Our business practices are being transformed. Security products are evolving. These changes must be a part of our strategic thinking for the future.

Changing threats and consequences: We are not fighting "pranksters" any more, but well financed and highly motivated criminals. We still must protect against e-mailed viruses, but are now more concerned about web-based malicious software, self-propagating worms, attacks on vulnerable applications, targeted phishing attacks, spyware, botnets and others. A driver for these changes is the improved marketability and usability of stolen personal and financial data. Consequences of a successful attack have changed from embarrassment or interruption in service to significant financial loss and issues of liability.

Changing business needs: Before, we concentrated on protecting our borders. Now we must let people in. Our primary customers for electronic services are no longer state employees, but citizens, organizations and business partners. To provide these services, we concentrate valued information in large databases linked to applications open to people all over the world. We must now pay close attention to server configuration, application security, system and application patches, authentication and authorization, malicious traffic and other things that may not have been big concerns before.

New tools and methods needed: We still need to filter out spam and e-mail viruses and install border protections. We must also filter out malicious web sites, apply patches quickly, develop secure applications, lock down desktops, implement secure configurations and remove unnecessary services from servers, use strong authentication, train employees, isolate data stores and more. Do we need automated traffic monitoring, outgoing traffic filtering, improved configuration management or other tools?

Vendor products, services and pricing are changing: There is a trend toward bundling security tools and requiring purchase of the bundle. Vendors are providing discounts when only their products are used, even when it is contrary to best practice; e.g. using two different antivirus vendor's products. Products we have used for years are no longer top performers. As product lines expand, support seems to decline. Vendors push for long-term contracts to lock customers in. There is little price competition, except with a large volume purchase. Vendors are generally getting better at identifying threats and quickly updating their products to stop them. Usually no clear "best" product or company surfaces and stays at the top. Core security products are becoming commodities with many customers changing products regularly, rather than staying with the same product year after year.

Security needs to be strategic: Security is not an extra cost add-on. It must become part of our core service-delivery requirements. Expecting all agencies to learn about, choose, implement, manage and maintain new security measures independently is inefficient and costly. We need to develop long-term strategies that accomplish goals and then figure out how to achieve them. Doing everything individually means we pay more (up front and TCO), can not take advantage of management efficiencies and can not help each other. Working collaboratively and strategically, we can improve security, reduce workloads and save money. It may also allow us to take advantage of opportunities that we can not individually.